WEB SERVER

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 6, Release 1

11 December 2006

Developed by DISA for the DoD

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
11 DEC 2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Web Server. Security Technical Implementation Guide. Version 6, Release 1	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defense Information Systems Agency,Arlington,VA,22202**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**67**	

This page is intentionally left blank.

TABLE OF CONTENTS

Page

LIST OF TABLES

TABLE OF FIGURES

This page is intentionally left blank.

SUMMARY OF CHANGES

Changes in this document since the previous release (Version 5, Release 1, dated 29 October 2004) are listed below.

GENERAL:

- Changed the version to Version 6, Release 0.
- Reorganized the document to address the general web server requirements in the main body of the STIG, and move the specific product implementation details to the associated companion checklist.

SECTION 1. INTRODUCTION

- Revised for improved clarity and technical correctness.

SECTION 2. GENERAL INFORMATION

Section 2.1 Web Server Security Administration

- Revised for improved clarity and technical correctness.
- Removed WA040
- Moved WA140 to new section 2.7, Web Server Backup and Recovery
- Added new requirement to require compliance with product specific configuration settings
    - *(WA000: CAT II) The SA will ensure the web server is configured in accordance with the product specific companion checklist.*

Section 2.4 Network Configuration

- Revised for clarity and additional content.
- Added new requirements based on network controls:
    - *(WG600: CAT I) The IAO will ensure only those ports specifically required to provide network access and web server functionality for the web server are open at the firewall.*
    - *(WG610: CAT II) The IAO will ensure web servers are configured to use only authorized ports and protocols in accordance with the Network Infrastructure STIG, DoD Instruction 8551.1, Ports, Protocols, and Services Management (PPSM) and the associated Ports, Protocols, and Services (PPS) Assurance Category Assignments List.*
    - *(WG620: CAT II) The IAO or SA will ensure a private web server using HTTPS has an Intrusion Detection System installed and operating.*

Section 2.5 Levels of Access Controls to Private Web Servers

- Revised for clarity and additional content.
- Removed WA080
- Added new vulnerability:
    - *(WG145: CAT II) The IAO will ensure a private web server using subscriber certificates, issued from any DoD aurthorized Certificate Authority, as an access control mechanism utilize an approved DoD certificate validation process.*

Section 2.7 Web Server Backup and Recover – New Section

SECTION 3. WEB SERVER SOFTWARE SECURITY

- Revised for clarity and additional content.
- Added additional vulnerabilities:
    - *(WA200: CAT II) The IAO will ensure the site has a formal migration plan for removing or upgrading web servers systems prior to the date the vendor drops security patch support.*
    - *(WA220: CAT II) The IAO will ensure compliance with all IAVM notices in coordination with the SA and Web Manager.*
    - *(WA230: CAT II) The IAO will ensure all software used with the web server has all related security patches applied and documented.*

Section 3.2 Service Packs and Patches

- Revised for clarity and additional content.
- Revised numbering of vulnerabilities.

Section 3.3 Installation

- Revised for clarity and additional content.
- Added vulnerability:
    - *(WG385: CAT I) The Web Managers or SAs will remove all documentation, sample code, example applications, and tutorials for middleware or the Web service from a production web server.*
- Replace WG090 with DS10.0140 from the Active Directory STIG.
    - *(WG090: CAT II) The Web Manager or SA will ensure a web server is not installed on the same platform as a Microsoft domain controller.*
    - *(DS10.0140: CAT III) The IAO will ensure Windows domain controllers are not utilized as hosts for applications including database servers, e-mail servers or clients, network address assignment (DHCP) servers, or web servers.*

Section 3.4 Configuration

- Moved Netscape specific checks to Netscape checklist.
- Moved WA170 to Software Security Section.

Section 3.6 Restrict Remote Authoring

- Added WG210.
- Provided alternative methods to remote post.
- Added vulnerabilities:
    - *(WG235: CAT I) The SA or Web Manager will ensure Remote authors or content providers are not able to upload files to the DocumentRoot directory without the use of a secure logon and secure connection.*
    - *(WG237: CAT I): The SA or Web Manager will ensure remote authors or content providers are not able to upload files to the DocumentRoot directory without being scanned to ensure no viruses or malicious code exists.*

Section 3.12 PKI Server Certificates

- Added vulnerability:
  - *(WG355: CAT II) The IAO will ensure a Private web server's list of Certificate Authorities considered trusted is limited to those with a trust hierarchy that leads to the DoD PKI Root Certificate Authority.*

Section 3.13 SSL/TLS

- Removed reference to superseded SecDef Memo dated 17 May 2001 Public Key Enabling of Applications.
- Revised references to SSL V3.0, clarified position on TLS vs. SSL V3.0 and NIST FIPS 140-2 Mode validation.

Section 4.5 Perl Scripts

- Provided options to starting a Perl script with the TAINT option.

Sections 4.14 and 4.15

- Moved to IIS Checklist.

Sections 4.6 JavaScript

- Moved the following checks to the Application Checklist.
  - *(WG480: CAT II) The Web Manager will ensure a JavaScript program is not used as the sole means of authentication.*
  - *(WG485: CAT II) The Web Manager will ensure a Java applet program is not used as the sole means of authentication.*

Section 5.1 File Transfer Protocol

- Changed SDID convention for FTP Vulnerabilities - WFTPxxx
- Added new vulnerability:
  - *(WFTP040: CAT II) The IAO will ensure anonymous FTP is not permitted on a "Private" web server.*

Section 5.3 Instant Messaging

- Removed.

Section 5.5 Web Application Servers

- Removed (now located in the Applications Services STIG).

Sections 5.6 Web Proxy Servers

- Added the following check:
  - *(WG560: CAT II) The IAO will ensure all external connections to Enclave level proxy servers are authenticated.*

APPENDIX A. RELATED PUBLICATIONS

- Added new publications and deleted those that no longer apply.

APPENDIX B. Netscape Server Configurations

- This section has been removed from the STIG and moved to the companion checklist.

APPENDIX C. UNIX Configuration
- This section has been removed from the STIG and moved to the companion checklist.

APPENDIX D. Microsoft IIS Configuration Details
- This section has been removed from the STIG and moved to the companion checklist.

APPENDIX E. Server Certificates
- This appendix is now Appendix B.

APPENDIX F. IBM HTTP Server (HIS) Websphere
- This section has been removed from the STIG and moved to the companion checklist.

APPENDIX G. IBM HTTP Server (HIS) for OS/390
- This section has been removed from the STIG and moved to the companion checklist.

APPENDIX H. Guidelines for Software Review of Vendor Provided Programs and Scripts
- This section has been removed from the STIG.

APPENDIX I. List of Acronyms
- This appendix is now Appendix C.

1. INTRODUCTION

Web servers provide access to data intended for a remote audience. This data may be intended for a restricted audience or it may be releasable to the general public. The web server must be capable of protecting the restricted data, as well as protecting data intended for a general audience. Immediate risks inherent to this role are external attack and accidental exposure. Although security controls such as firewalls, Intrusion Detection Systems (IDSs), and baseline integrity checking tools offer some defense against malicious activity, security for web servers is best achieved through a comprehensive defense-in-depth strategy. This strategy includes, but is not limited to, server configuration to prevent system compromise, operational procedures for posting data to avoid accidental exposure, proper placement of the server within the network infrastructure, and the allowance or denial of ports, protocols, and services used to access the web server. The purpose of this STIG is to assist Department of Defense (DoD) sites in planning web server deployment and securing already-deployed web servers in an effort to achieve the minimum requirements, standards, controls, and options for secure web server operations.

This STIG, in conjunction with its companion documents, the Web Server Checklists, provides the guidance to assist with the task of implementing security on a variety of web server platforms. This STIG, combined with the appropriate Operating System (OS) STIG and other technology-specific STIGs, provides a comprehensive approach to web server security. The contents of this STIG are intended to facilitate the security research, planning, design, installation, deployment, and operational maintenance of the web server lifecycle. Specific security configuration guidance for the Netscape/iPlanet/Sun JAVA System Server, Apache, and Microsoft Internet Information Server (IIS) applications can be found in the companion Web Server Checklists, which are external to this STIG.

1.1 Background

Since web servers provide data via an externally or publicly exposed interface, the web server is a well-known target for exploitation. Unprotected web servers provide an avenue for malicious activity, such as theft or the denial of service to an organization's resources. This is consistent with a trend in malicious user behavior, which focuses on attacking applications accessible via the Internet, as opposed to attacking the operating system of the host platform. An improperly configured web server can be attacked directly and be used as a staging area to obtain unauthorized access to an organization's internal resources.

Major security forums (e.g., SysAdmin, Audit, Network, Security (SANS) Institute and the Open Web Application Security Project (OWASP)) publish reports describing the most critical Internet security threats. From these reports, some threats unique to web server technology are as follows:

- Non-existent Anti-Virus Applications or outdated definitions
- Instant Messaging (IM) Applications
- Default OS and web server software installs and mis-configurations
- Broken access controls, accounts with no passwords, weak passwords, or default passwords
- Unvalidated input

- Cross site scripting
- Broken authentication and session management
- Non-existent or incomplete backups
- Non-existent or incomplete logging
- Vulnerable common gateway interface (CGI) programs and application extensions installed on web servers
- Remote data services in Microsoft IIS
- Global file sharing and inappropriate information sharing via NetBIOS and Windows ports 135 – 139 (port 445 in Windows 2000), UNIX NFS exports on port 2049, and Macintosh web sharing (AppleShare/IP) on ports 80, 427, and 548

1.2 Authority

DoD Directive 8500.1 requires that "all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines" and tasks DISA to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA." This document is provided under the authority of DoD Directive 8500.1.

The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DoD systems operating at the Mission Assurance Category (MAC) II Sensitive level, containing sensitive information.

The Information Operations Condition (INFOCON) for the DoD recommends actions during periods when a heightened defensive posture is required to protect DoD computer networks from attack. The IAO will ensure compliance with the security requirements of the current INFOCON level and will modify security requirements to comply with this guidance.

It should be noted that Field Security Operations (FSO) support for the STIGs, Checklists, and Tools is only available to DoD Customers.

1.3 Scope

The requirements in this document will assist Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), Security Managers (SMs), System Administrators (SAs) and Web Managers in securing web server technologies. This document will also assist in identifying external security exposures created when the site is connected to at least one Information System (IS) outside the site's control. This document does not address issues related to style, performance, response time, or bandwidth.

This STIG addresses known security issues inherent to web server technologies. Although web server technologies vary between vendors, most web server platforms provide a means for implementing the security requirements contained herein. General web server requirements are furnished in the main body of this document while platform and product-specific requirements are provided in the companion checklists.

There are many functional areas of Internet and Intranet web technology that must be secured, including the following:

- Network access - architecture
- The host operating system
- Web server software
- The application running via the web server, to include associated scripts and data
- The database server and associated applications
- Information (e.g., account logon data) that is transmitted between client and server

This STIG addresses the web server software security issues while the other areas in the above list are addressed in companion STIGs to include: Network Infrastructure, Application Services, Application Security and Development, Database, and Operating Systems STIGs.

This document provides the technical security policies, requirements, and implementation details for applying security concepts to web servers.

1.4 Writing Conventions

Throughout this document, statements are written using words such as "**will**" and "**should**". The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses "**will**" indicates mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This makes all "**will**" statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written.

A reference to "**should**" indicates a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. Nevertheless, all reasonable attempts to meet this criterion will be made.

For each italicized policy bullet, the text will be preceded by parentheses containing the STIG Identifier (STIGID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this will be as follows: "(*G111: CAT II*)." If the item presently does not have an STIGID, or the STIGID is being developed, it will contain a preliminary severity code and "N/A" (i.e., "*[N/A: CAT III]*").

1.5 Vulnerability Severity Code Definitions

Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall. These can lead to the immediate compromise of the web server allowing the attacker to take complete control of the web server and associated operating system, which can then be used as a resource to control other systems in your network. Some examples would be the running of unsupported software, anonymous access to privledge accounts, and the presence of sample applications installed on the web server.
Category II	Vulnerabilities aide the ability of an attacker to gain access into a machine, compromise sensitive data, or bypass a firewall. These will lead to the eventual compromise of the web server allowing the attacker to manipulate the content or server settings on the web server and have access to other systems in your network. Some examples would be trust relationships with unauthorized separate enclaves, non compliance with appropriate host operating system security controls, and the non compliance with the IAVM program.
Category III	Vulnerabilities that impact the security posture of the system and if configured, will improve the overall security of asset. These could result in the degradation of service, compromise of information, and in some cases lead to unauthorized access to the system. Some examples would be untrained staff, development tools on a production environment, and the uncontrolled release of information to the web server.

Table 1-1. Vulnerability Severity Codes

1.6 DISA Information Assurance Vulnerability Management (IAVM)

The DoD has mandated that all IAVMs are received and acted on by all commands, agencies, and organizations within the DoD. The IAVM process provides notification of these vulnerability alerts and requires that each of these organizations take appropriate actions in accordance with the issued alert. IAVM notifications can be accessed at the Joint Task Force - Global Network Operations (JTF-GNO) Web site, https://www.jtfgno.mil.

1.7 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) Web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information. The NIPRNet URL for the IASE site is http://iase.disa.mil/.

1.8 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to fso_spt@disa.mil. DISA FSO will coordinate all change requests with the relevant DoD organizations before inclusion in this document.

This page is intentionally left blank.

2. GENERAL INFORMATION

2.1 Web Server Security Administration

The SA is responsible for the host operating system. Web administrative responsibilities are assigned to the Web Manager or equivalent position, and include one or more of the following security responsibilities:

- Configure and manage the web server in accordance with this STIG and IAO guidance.
- Coordinate placement of information and scripts on the web server with appropriate authorities.
- Provide security guidance and training to personnel regarding the capabilities and features of the web server.
- Advise the IAO of any technical, operational, or security problems along with possible solutions.

A separate web administrators group is suggested for the assignment of the web server administration tasks. This will allow for greater granularity in the control and assignment of these responsibilities.

- *(WA050: CAT III) The IAO will ensure trained staff (i.e., a Web Manager and a System Administrator) are appointed for each web server.*

NOTE: The Web Manager may be an additional duty or a separate role.

There are specific product dependent settings and controls that will need to be configured to ensure the secure configuration of the web server. Because these controls do not apply to every web server product, the specifics are documented in the associated product specific companion checklist.

- *(WA000: CAT II) The SA will ensure the web server is configured in accordance with the product specific companion checklist.*

The organization or activity that sponsors the web site will have web content responsibility. These persons will ensure that all information is kept current and that information and scripting placed on the web server is reviewed and approved by a configuration management authority.

- *(WA030: CAT II) The IAO or IAM will verify local policies are developed to ensure all information posted is reviewed and approved by appropriate authorities and as needed by the Public Affairs Officer (PAO) prior to release.*

- *(WA035: CAT II) The IAO or IAM will verify local policies are developed to ensure all information that is hosted on a DoD site, which originated from a DoD or other Federal organization, is reviewed and approved for posting by the originating organization according to the Web Site Administration Policies and Procedures, dated 25 November 1998.*

2.2 Recommended Process for Content Approval and Posting

Much coordination and cooperation is involved in crafting and obtaining approval for the placement of information on a DoD web site. A communications method, such as email, should be used as the means of notification that files are ready for placement on the web server. The objective is to verify the organization or program's web page guidelines for posting new content have been followed.

In cases where content is generated from a database or approved web application via an interactive user session, the system through which the database is populated or through which the application generates content, operates under an approved process inherent to the system in question.

The easiest method for obtaining content approval is to view pending content via a web browser. The author should notify appropriate managers of the file location via email. Several areas of content requiring evaluation include, but are not limited to the following issues:

- Testing by organizational Webmaster and/or alternate
- Validation of author's functional testing
- Validation of file names and locations
- Review of content for potential issues
- Review and approval by the organizational content manager and configuration management authority

After the pending content is organizationally and technically approved, the organizational Web Content Manager should forward the files to the appropriate command representative or Office of Public Affairs as appropriate for subsequent review.

When submitting materials for review/approval, the following information should be submitted:

Web Page Posting Request

Name of Organizational Content Manager: __Jane Dough_____

Department/Organization: __Web Managmeent (WB04)_____

Telephone Number (direct line): _111.222.1234_____

Name of Page Author: (If applicable) ___Sally Skript_____

To be Posted on: Intranet (Server_name) [X] Internet (server_name.mil) [ ]

Password protected: YES [X] NO [ ]

Pubic Key Infrastructure (PKI) enabled: YES [X] NO [ ]

FOUO document: YES [X] NO [ ]

Content: _____Software Release Schedule_____

Web Site URL: _www.samplesite.mil_____

New Page[ ] Revision[X] Major Change[ ] (List in the "Comments" section)

Specific files/documents to be reviewed: (List separately) release.html

Comments: Call if you have any questions

2.3 Private and Public Web Servers

A DoD private web server as defined by the *Department of Defense Instruction 8520.2 is:*

"E2.1.12. DoD Private Web Server. For unclassified networks, a DoD private web server is any DoD-owned, operated, or controlled web server providing access to sensitive information that has not been reviewed and approved for release in accordance with DoD Directive 5230.9 (reference (q)) and DoD Instruction 5230.29 (reference (r)). For Secret Internet Protocol Router Network and other classified networks that are not accessible to the public, a DoD private web server is any server that provides access to information that requires need-to-know control or compartmentation."

A DoD public web server is any DoD-owned, operated, or controlled web server providing access to information that has been reviewed and approved for release in accordance with DoD Directive 5230.9 and DoD Instruction 5230.29.

Given the DoD definition of a private web server, a public web server may reside on the SIPRNet provided that the information published does not require need-to-know control or compartmentation.

While posting appropriate data to a properly protected public or private web server is necessary to facilitate operations, all personnel and other content providers must exercise extreme caution to ensure that they do not post inappropriate material. Current examples of such material include classified data; data covered by the Privacy Act, unclassified but sensitive data (such as Health Insurance Portability and Accountability Act (HIPAA) related information), contract (procurement) sensitive information, proprietary data, or For Official Use Only (FOUO) information.

2.4 Network Configuration

Web servers within the DoD can be designated as either public or private. Web servers supporting public information are highly visible targets for malicious users. From a network perspective, the following controls are relevant:

- Premise Router Filtering
- Intrusion Detection
- Firewall protection
- Connections to internal hosts and support servers

Public web servers must be isolated from internal systems. Public web server also refers to web servers that may be located on non-public networks and that contain information that is approved for release to the entire community. Public web servers must not have trusted connections with assets outside the confines of the demilitarized zone (DMZ) or isolated separate public enclave

(subnet). This trusted connection is not to be confused with a Microsoft Domain trust. A trusted connection can be an attachment to Microsoft shares, in UNIX as Network File System (NFS) mounts, as well as connections to interior enclave printers. This relationship can also be found with connections from public web servers to interior enclave databases.

Private web servers, which host sites that serve controlled access data, must also be protected from outside threats in addition to insider threats. Insider threat may be accidental or intentional, but in either case, can cause a disruption in service of your web server. To protect the private web server from these threats, it must be located on a separate controlled access subnet and not part of the public DMZ that houses the public web servers. It also cannot be located inside the enclave as part of the local general population LAN.

In addition, systems requiring greater assurance for availability (MAC I and MAC II) should have the web server located on a separate server than that of the database or other application. This helps to minimize any security events to the compromised system. Encryption requirements, for data transmitted between these systems, is dependent on the sensitivity of the data being transmitted, the sensitivity level assigned to the network being traversed, and any differences in need-to-know between the data and the users on the network. Login credentials to the Database Management System (DBMS) and web servers will always be encrypted. All encryption will use Federal Information Processing Standards (FIPS) 140-2 validated cryptography. Please consult the DISA *Enclave STIG* and DISA *Network Infrastructure STIG* for detailed networking requirements.

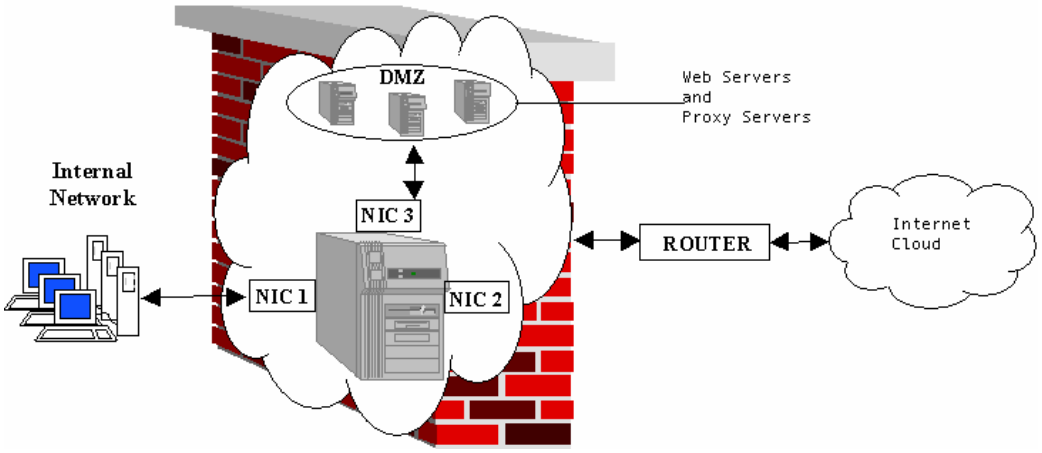

Figure 2-1. Typical Web Server DMZ

- *(WA060: CAT II) The IAO will ensure a public web server is isolated in accordance with the Network Infrastructure STIG. A public web server is on a separate subnet isolated from the internal systems.*

- *(WA070: CAT II) The IAO will ensure a private web server is located on a separate controlled access subnet.*

- *(WG600: CAT I) The IAO will ensure only those ports specifically required to provide network access and web server functionality are open at the firewall.*

- *(WG610: CAT II) The IAO will ensure web servers are configured to use only authorized ports, protocols, and services in accordance with the Network Infrastructure STIG, DoD Instruction 8551.1, Ports, Protocols, and Services Management (PPSM) and the associated Ports, Protocols, and Services (PPS) Assurance Category Assignments List.*

- *(WG620: CAT II) The IAO or SA will ensure a private web server using HTTPS has an IDS installed and operating.*

- *(WG040: CAT II) The SA will ensure a public web server does not have a trusted connection with any asset external to its public enclave.*

***NOTE*:** This check does not imply a "Trust" as defined by a Microsoft Domain.

2.5 Levels of Access Controls to Private Web Servers

The *DoD Web Site Administration Policies and Procedures*, dated 25 November 1998 and *DoD Instruction 8520.2*, define access controls for private web servers based on the sensitivity of the information that will be accessed and the target audience for that information. They also provide guidance on the technology that will be used to obtain the appropriate level of protection. These technologies include, but are not limited to, Internet Protocol (IP) address/domain name restriction, user ID/password requirements, Secure Sockets Layer/Transport Layer Security (SSL/ TLS) and PKI (see Section 3.13). The Program Manager (PM), in coordination with the IAO, will determine which technology or combination of technologies will be applied to a particular web server.

Private web servers will be protected from unauthorized remote access at the enclave perimeter and host levels.

- *(WA025: CAT II) The IAO will document the sensitivity level of all data for publication on a production web server.*

- *(WG140: CAT II) The IAO will ensure private web servers require subscriber certificates, issued from any DoD aurthorized Certificate Authority as an access control mechanism for users.*

- *(WG145: CAT II) The IAO will ensure a private web server using subscriber certificates, issued from any DoD aurthorized Certificate Authority, as an access control mechanism utilizes an approved DoD certificate validation process.*

CONTROLS	*SECURITY*	*DATA SENSITIVITY*
Public - Access can be controlled by IP address or some other means where the restriction is not due to data sensitivity.	Unencrypted	Non-sensitive, of general interest to the public, cleared and authorized for public release for which worldwide dissemination poses limited risk for DoD or for DoD personnel, even if aggregated with other information reasonably expected to be in the public domain
Private – User PKI certificate Server PKI certificate	Encrypted SSL	Sensitive information that has not been reviewed and approved for release in accordance with DoD Directive 5230.9 (reference (q)) and DoD Instruction 5230.29 (reference (r))

Table 2-1. Minimum Web Server Access Control Requirements

2.6 Passwords

Some web-based applications utilize the use of user IDs and passwords. In some cases these passwords are OS accounts and provide remote user access to other applications or databases. In this situation, the OS password policy applies. In other instances, the user ID and password scheme is determined by the application. In this case, the application's documentation should detail the policy to be followed to add users and select or change passwords. Files containing sensitive password information should be owned by the SA or Web Manager account and reflect the minimum permissions necessary to allow the application to function as documented.

In cases where a Lightweight Directory Access Protocol (LDAP) server is used for authentication, the procedures for the web server suite should detail the web site's password policy.

A private web server controls access by allowing only authorized users. Private web servers will have a connection restriction policy established to deny access to all except specifically authorized hosts or subnets. In addition, private web servers are required to utilize approved DoD subscriber certificates for authentication and not rely solely on userids and passwords.

The user may change passwords for web applications but the logon and password management screens must be encrypted with a minimum of 128-bit SSL/TLS encryption. Forgotten passwords should not be sent via email to the user, but rather a process for chaning the forgotten password should be followed. Password policies to include password strength will comply with the appropriate operating system STIG.

- *(WA150: CAT II) The IAO will ensure web applications or servers, which require restriction by user ID and password, require web users to have a user ID and password that provide access only to the web content.*

NOTE: Shared user accounts are not authorized.

- *(WG050: CAT II) The IAO will ensure the web server password is entrusted to the SA or Web Manager.*

- *(WG060: CAT II) The SA or Web Manager will ensure the web server application or system password is changed at least annually.*

2.7 Web Server Backup and Recovery

A tested and verifiable backup strategy will be implemented for web server software as well as all web server data files. Backup and recovery procedures will be documented and the Web Manager or SA for the specific application will be responsible for the design, test, and implementation of the procedures.

The site will have a contingency processing plan/disaster recovery plan that includes web servers. The contingency plan will be periodically tested in accordance with DoDI 8500.2 requirements.

The site will identify an off-site storage facility in accordance with DoDI 8500.2 requirements. Off-site backups will be updated on a regular basis and the frequency will be documented in the contingency plan.

- *(WA140: CAT III) The IAO will ensure web server content and configuration files are part of a routine backup program in order to recover from file damage and system failure.*

This page is intentionally left blank.

3. WEB SERVER SOFTWARE SECURITY

This section identifies the policies and requirements that must be followed when implementing a web server. A good plan will address items such as proper hardware selection, software configuration on the server, components to be installed, and security controls to be used. Prior to the installation of any web server software, the host operating system will be configured in accordance with the appropriate STIG.

- *(WA160: CAT II) The Web Manager or SA will ensure before installing the web server application, the server host platform operating system is configured in accordance with the appropriate OS STIG as well as the Enclave STIG.*

- *(WG190: CAT I) The Web Manager or SA will ensure the web server application software is a version supported by the vendor and appropriate to the host OS of the server.*

- *(WA200: CAT II) The IAO will ensure the site has a formal migration plan for removing or upgrading web servers operating systems prior to the date the vendor drops security patch support.*

A DoD computing system, which refers any technology asset or application, is required to comply with all IAVM notices that are issued. These notices address specific security vulnerabilities that have been identified as significant threats to the web server environment. The IAVM process does not address all patches that have been identified for the host operating system, or in this case, the web server software environment. Many vendors have subscription services available to notify users of known security threats. The site needs to be aware of these fixes and make determinations based on local policy and what software features are installed, if these patches need to be applied. In some cases, patches also apply to middleware and database systems. Maintaining the security of web servers requires frequent reviews of security notices. Many security notices mandate the installation of a software patch to overcome security vulnerabilities.

SAs and IAOs should regularly check the OS and application software vendor web sites for information on new security patches that are applicable to their site. All applicable security patches will be applied to the operating system and web server software. Security patches are deemed applicable if the product is installed, even if it is not used or is disabled.

FSO does not test or approve patches or service packs. It is the site's responsibility to test vendor patches within their test environment.

- *(WA220: CAT II) The IAO will ensure compliance with all IAVM notices in coordination with the SA and Web Manager.*

- *(WA230: CAT II) The IAO will ensure all software used with the web server has all related security patches applied and documented.*

NOTE: If problems are discovered with the software patch during testing, the IAO will ensure that the vendor is contacted to remedy the issue.

In the event that an unexpected occurrence disrupts the web server's function, a mechanism will be in place to guide the SA or Web Manager through the process of determining the cause and effect of such an event. This will involve the use of forensic techniques such as log file research as well as file and directory modification analysis.

- *(WA170: CAT II) The IAO will ensure procedures are in place that require the SA or Web Manager to investigate any unscheduled or unanticipated disruption to the web service.*

3.1 Open Source Software

DoD has clarified policy on the use of open source software to take advantage of the capabilities available in the Open Source community as long as certain prerequisites are met. DoD no longer requires that OS software be obtained through a valid vendor channel and have a formal support path, if the source code for the OS is publicly available for review, and the conditions listed below are met.

DoD CIO Memo, "Open Source Software (OSS) in Department of Defense (DoD), 28 May 2003:"

"DOD Components acquiring, using or developing OSS must ensure that the OSS complies with the same DoD policies that govern Commercial off the Shelf (COTS) and Government off the Shelf (GOTS) software. This includes, but is not limited to, the requirements that all information assurance (IA) or IA-enabled IT hardware, firmware and software components or products incorporated into DoD information systems whether acquired or originated within DoD: Comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy Number 11 and be configured in accordance with DoD-approved security and configuration guidelines at http://iase.disa.mil/ and http://www.nsa.gov/."

Open source software:

1. A utility that has publicly available source code is acceptable.
2. A commercial product that incorporates open source software where the commercial vendor provides a warranty is acceptable.
3. Vendor supported open source software is acceptable.
4. Open source software that provides security patch support and verified source code is acceptable.

3.2 Service Packs and Patches

Web server software is periodically updated with vendor patches and fixes. These patches address security vulnerabilities that have been discovered on systems that have been compromised, as well as by routine updates from the vendor.

3.3 Installation

To ensure a secure and functional web server, a detailed installation and configuration plan should be developed and followed. This will eliminate mistakes that arise as a result of ad hoc decisions made during the default installation of a server. Planners should not attempt to support multiple services such as Domain Name Service (DNS), e-mail, databases, search engines, and indexing or streaming media on the same server that is providing the web publishing service. In order to take full advantage of these services, it is normally necessary, and recommended, to install them on separate servers.

In the case of File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and Network News Transport Protocol (NNTP), a well-defined need for these services should be documented by the IAO prior to their installation on the same platform as a web server. Primary and secondary Domain Controllers, in the Windows environment, will not share a common platform with a web server World Wide Web (WWW) service.

In the case of a web server supporting multiple applications, such as 3 unique web sites for 3 unique organizations, it is acceptable to support this type of configuration. In this situation, each of the unique applications should be installed in their own, unique, document directory which is part of a unique installation of the web site. This will allow the web server to support differing components for each of the applications and provide some flexibility to application owners. It should also be noted that all the applications that are being supported in this configuration must have the same data protection requirements. A web server cannot be supporting both public and private web sites. This would violate the trusted connection requirement.

- *(WG204: CAT II) The IAO will ensure, if approved for installation, each installed Internet service (e.g., WWW, FTP, SMTP, and NNTP) is located on a separate partition or drive.*

- *(DS10.0140: CAT III) The IAO will ensure Windows domain controllers are not utilized as hosts for applications including database servers, e-mail servers or clients, network address assignment (DHCP) servers, or web servers.*

Compilers and utility programs, such as office suites, graphic editors, third-party text editors, middleware development tools, and script editing GUIs, will not be permitted on production web servers. Software that supports development work shall not be installed on a production server. However, vendor software may require JAVA Runtime Environment (JRE), JAVA Development Kit (JDK), or Software Development Kit (SDK) for Java support. JDK will be allowed on production servers to meet this requirement.

- *(WG080: CAT II) The Web Manager or SA will ensure if compilers are installed on a production web server they are restricted to Administrators only.*

- *(WG130: CAT III) The Web Manager or SA will ensure utility programs, traditional workstation applications, or development tools are not installed on the same platform as the production web server.*

Finally, delete all directories that contain "samples" and any scripts used to execute the "samples". As an example, the following is a list of directories created during the installation of IIS. It is recommended that these directories be deleted. If there is a requirement to maintain these directories at the site on non-production servers for training purposes, etc., have NTFS permissions set to only allow access to authorized users, i.e., Web Admins and Administrators.

\%systemcontent%\InetPub\iissamples
\%systemcontent%\InetPub\Scripts\Samples
\%systemcontent%\InetPub\AdminScripts

- *(WG385: CAT I) The Web Managers or SA will remove all web server documentation, sample code, example applications, and tutorials from a production web server.*

3.4 Configuration

This section provides the policies and requirements regarding the secure configuration of the web server host platform OS. The term 'superuser' refers to the user ID that has no access restrictions on the host platform. For instance, in UNIX, the superuser would be the root account; in Windows, the superuser account would be the Administrator account or an account with administrative privilege. The policies in this section are applicable to both public and private web servers unless specifically addressed.

At this time, a web server configured according to the vendor's defaults will not meet the required security standards of this document. For example, a default installation setting for Netscape web servers is that automatic directory indexing is enabled. Such a setting makes it easy for malicious users to gather information about the configuration of the web server. In the case of IIS, default file extensions must be removed, and support for unlimited connections and FTP services must be disabled.

To help secure the web server, security controls above and beyond the defaults need to be implemented. This will enhance the security controls that have already been implemented in accordance with the appropriate OS STIG.

- *(WG135: CAT II) The Web Manager or SA will ensure unnecessary services are disabled on the web server.*

This check verifies that the web server is not configured to permit an unlimited number of HTTP requests. When this parameter is set to "unlimited", this facilitates a denial of service attack.

- *(WG110: CAT II) The Web Manager will ensure the number of simultaneous requests that a web server allows is not set to unlimited.*

The web server response header of an HTTP response can contain several fields of information including the requested HTML page. The information included in this response can be web server type and version, operating system and version, and ports associated with the web server. This provides the malicious user valuable information without the use of extensive tools.

- *(WG520: CAT III) The Web Manager or SA will ensure the advertising of information pertaining to the operating system version, web server type and version, and web server ports is restricted on public web servers.*

The goal is to completely control the web users experience in navigating any portion of the web document root directories. Ensuring all web content directories have at least the equivalent of an "index.html" file is a significant factor to accomplish this end. Also, enumeration techniques, such as URL parameter manipulation, rely upon being able to obtain information about the web server's directory structure by locating directories without default pages. This practice helps ensure that the anonymous web user will not obtain directory browsing information or an error message that reveals the server type and version. This will be accomplished using the "Deny All" allow list feature and a robots.txt file in the document root directory.

NOTE: The robots.txt file is an informal standard that was developed in the mid 1990's to provide the web owner a mechanism to exclude the web robot, spider or crawler from gathering information about linked pages on their web sites.

- *(WG170: CAT II) The Web Manager will ensure each readable web document directory contains a default, home, index, or equivalent file.*

- *(WG310: CAT III) The IAO will ensure a public web server does not respond to calls by public search engines.*

NOTE: This includes web message board and collaboration servers.

3.5 Access Controls

Many of the security problems that occur are not the result of a user gaining access to files or data for which the user does not have permissions, but rather users are assigned incorrect permissions to unauthorized data. The files, directories, and data that are stored on the web server need to be evaluated and a determination made concerning authorized access to information and programs on the server.

In most cases we can identify several types of users on a web server. These are the system SAs, Web Managers, auditors, authors, developers, and the clients (web users, either anonymous or authenticated). Only authorized user and administrative accounts will be allowed on the host server in order to maintain the web server, applications, and review the server operations.

The Defense Originating Office (DOO), in accordance with the guidance provided in *Web Site Administration Policies and Procedures*, dated 25 November 1998 updated January 2002, initially defines these controls. The Web Manager for the web site will need to know the user community and data sensitivity (defined by the data owner) to define access restrictions for the content. Once identified, the required controls should be documented in such a manner as to address items such as who is allowed access, which persons are responsible for security, and what the process is for making changes to the web server.

The SA and Web Manager will often work together to install and configure the web server software. The authors and developers design the web pages. Auditors monitor performance, trouble-shoot and look for breaches of security. The client uses the resources provided on the web server. Permissions on directories and subdirectories will be set to restrict access applying the least privilege principle for operational use.

- *(WG195: CAT I) The SA will ensure any anonymous access account is not a privileged account or a member of any group with privileged access.*

- *(WG220: CAT II) The SA or Web Manager will ensure access to the web administration tool is restricted to the Web Manager and the Web Manager's designees.*

- *(WG230: CAT I) The IAO will ensure the SA or Web Manager performs all administrative tasks through a secure, encrypted path.*

3.6 Restrict Remote Authoring

Remote web authors should not be able to upload files to the DocumentRoot directory structure without virus checking and checking for malicious or mobile code. A remote web user whose agency has a Memorandum of Agreement (MOA) with the hosting agency and has submitted a DoD form 2875 (*System Authorization Access Request* (SAAR)) or an equivalent document will be allowed to post files to a temporary location on the server. All posted files to this temporary location will be scanned for viruses and content checked for malicious or mobile code. Only files free of viruses and malicious or mobile code will be posted to the appropriate DocumentRoot directory.

- *(WG235: CAT I): The SA or Web Manager will ensure remote authors or content providers are not able to upload files to the DocumentRoot directory without the use of a secure encrypted logon and secure encrypted connection (FIPS 140-2 validated for FIPS Mode use).*

- *(WG237: CAT I) The SA or Web Manager will ensure remote authors or content providers are not able to upload files to the DocumentRoot directory without being scanned to ensure no viruses or malicious code exists.*

Web content directories are network sharable. Such sharing is a security risk when a web server is involved. Users accessing the share anonymously could experience privileged access to the content of such directories. Network sharable directories expose those directories and their contents to unnecessary or unauthorized access. Any unauthorized exposure increases the risk that someone could exploit that access and either compromise the web content or cause web server performance problems. NIST Guidelines for Securing Public Web Servers (par. 8.6 pg. 75, a principle reference for this document) states "Do not mount any file shares on the internal network from the web server or vice versa".

- *(WG210: CAT II) The SA will ensure the web document root (web content directory) is not sharable, NFS mounted, or exported to partitions on a Private network.*

Alternative methods must be found to provide connectivity for remote authoring. One such method is the use of an Out-of-Band (OOB) administrative network. Another approach would be the use of a point-to-point virtual private network (VPN) solution. Both approaches would require the use of remote control software or secure shell. This alleviates the need to open restricted ports such as the NetBIOS ports 137, 138, and 139 used to advertise Microsoft shares.

3.7 Web Log Files and Banner Page

3.7.1 Log Files

By reviewing log files SAs, Web Managers, and Auditors can determine site access, web resources requested, the scope and pattern of web site traffic, and the difficulties the server might be experiencing serving requests. The minimum items to be logged to achieve this are as follows:

- User ID
- Date and time of the event
- Type of event
- Source
- Success or failure of the event
- Successful and unsuccessful logons
- Starting and ending of access time for access to the system
- URI Query
- HTTP Status
- Referrer

- *(WG242: CAT II) The SA or Web Manager will ensure log file data include the following: Date, Time, Client IP Address, User Name, HTTP Method, URI Query string, Http Protocol Status, and Referrer. These log items are created in the event of:*

  - Successful and unsuccessful attempts to access the web server software.
  - Successful and unsuccessful attempts to access the web site.
  - Successful and unsuccessful attempts to access the web application.

The DoD 8500.2 states, “ECRR-1 Audit Record Retention - If the DoD information system contains sources and methods intelligence (SAMI), then audit records are retained for 5 years. Otherwise, audit records are retained for at least 1 year.”

- *(WG240: CAT II) The SA or Web Manager will ensure logs of web server access and errors are established and maintained.*

- *(WG250: CAT II) The SA or Web Manager will ensure auditors are the only users with greater than read access to log files.*

- *(WG255: CAT II) The SA or Web Manager will ensure access to the web server log files is restricted to Administrators, the user assigned to run the web server software, and Auditors.*

NOTE: This does not apply to active log files that require the system account to have full access.

- *(WA110: CAT III) The IAO will ensure web server log files are retained for a period of 1 year.*

3.7.2 Recommended Banner Page with Logging Policy

A consent banner will be in place to make prospective entrants aware that the web site they are about to enter is a DoD web site and their activity is subject to monitoring. Section 4 of the *DoD Web Site Administration Policies and Procedures Guide* has a sample consent banner that can be tailored by your organization. The consent banner is required to contain the following five notifications: the system being a DoD system, the system is subject to monitoring, the use of the system constitutes consent to monitoring, the system is for authorized U.S. Government use only, and that monitoring is authorized in accordance with the applicable laws and regulations and conducted for purposes of systems management and protection, protections against improper or unauthorized use or access, and verification of applicable security features or procedures.

- *(WG265: CAT II) The IAO or Web Manager will ensure an approved banner page is in place. The banner must include the following five elements:*

  - *The system is a DoD system.*
  - *The system is subject to monitoring.*
  - *Monitoring is authorized in accordance with the applicable laws and regulations and conducted for purposes of systems management and protection, protections against improper or unauthorized use or access, and verification of applicable security features or procedures.*
  - *Use of the system constitutes consent to monitoring.*
  - *The system is for authorized U.S. Government use only.*

3.8 Development Web Servers

It is recognized that in some instances, web site development for a web server must take place in an environment that replicates the ultimate physical and logical location of the web server. The preferred solution to this challenge is a test environment that simulates the production environment.

The main concern in this case is the risk to other servers located on the same subnet. Thus, providing a separate subnet for this server is recommended. A development web server installation should be documented and approved by the PM, IAM, or IAO.

Development servers will comply with the standards set forth in this STIG and the STIG for the host OS.

- *(WG260: CAT III) The SA or Web Manager will ensure web sites still under development do not exist on a production server.*

3.9 Classified Web Servers

When data of a classified nature is migrated to a web server, fundamental principles applicable to the safe guarding of classified material must be followed.

The SA or Web Manager will ensure the content of a classified web server exhibit proper labeling on each screen, be it a static page or dynamically generated page that is appropriate to the classification of the system's content.

- *(WA155: CAT II) The IAO will ensure a classified web server is afforded physical security commensurate with the classification of its content (i.e., is located in a vault or room approved for classified storage at the highest classification processed on that system).*

3.10 File and Directory Access Rights for Web Servers

In addition to OS restrictions, access rights to files and directories can be set on a web site using the web server software. That is, in addition to allowing or denying all access rights, a rule can be specified that allows or denies partial access rights. For example, users can be given read-only access rights to files, to view the information but not change the files.

- *(WG270: CAT II) The SA or Web Manager will ensure on web servers, the* htpasswd *file (if present) is owned by the SA or Web manager and has permissions of owner: read/write, group: read, and others: none (550). Equivalent permissions in a Windows environment are Administrators, System, and the user defined to run the web server software full control.*

- *(WG280: CAT II) The SA or Web Manager will ensure on web servers, the access control files, for example the .htaccess and .nsconfig files, are owned by a non-privileged web server account and have permissions of owner: read, group: none, and others: none (400 in a UNIX environment and Administrator and System full control in a Windows environment).*

- *(WG290: CAT I) The SA or Web Manager will ensure the web client account (i.e., IUSR_machinename, anyone, or nobody) has access to the content and necessary scripts directory structure. Access is limited to read and where necessary execute. (In the case of IIS 4.x/5.x, execute equates to script as configured in the Microsoft Management Console (MMC).)*

NOTE: If the Web Manager group account has been authorized by the IAO to update and maintain the access control file, the permissions would be owner: read, group: read/write, others: none (460). (Such uneven permissions will be documented.)

- *(WA120: CAT III) The Web Manager will document the administrative users and groups that have access rights to the web server.*

- *(WG205: CAT II) The SA or Web Manager will ensure all web server system files (web server root) are placed in a separate directory or partition from the web server document directory(ies) (web document root).*

- *(WG275: CAT II) The SA will ensure the web server, although started by superuser or privileged account, is run using a non- privileged account.*

NOTE: This does not apply to IIS versions that do not support alternate accounts.

- *(WG300: CAT II) The IAO will ensure web Server system files conform to minimum file permission requirements.*

3.11 Microsoft Operating Systems

In some cases, currently installed hotfixes and or patches can be rendered invalid when an update is made to middleware or other software products from a third-party software vendor.

After a security patch installation, the hotfix "Q" number can be found in the system registry. If server software such as Cold Fusion, Crystal Reports, or even an additional IIS plug-in is installed, certain files in the c:\%systemroot%\system32\inetsrv directory can be overwritten. When this happens, the vulnerability that the patch fixed reverts back to the original state, thus making the system vulnerable again. The registry will still show the "Q" number as being installed; however, the actual data on the drive has been altered.

Installations that can possibly affect the previously installed patches are as follows:

- Any IIS/MMC type software that utilizes plug-ins and or accesses systemroot/inetsrv information
- Web reporting software
- In Windows 2000, running the Add/Remove Windows Components screen regarding IIS (to include reinstalling IIS)

3.12 PKI

The PKI supports the following services:

- Establishment of domains of trust and governance
- Confidentiality (encrypting)
- Integrity and authentication (signing)
- Non-repudiation service
- End-to-end monitoring, reporting, and auditing of PKI services

See *Appendix B, Server Certificates,* of this document for detailed instructions for obtaining server certificates.

3.12.1 PKI Server Certificates

A PKI certificate is a digital identifier that establishes the identity of an individual or a platform. A server that has a certificate provides users with third-party confirmation of authenticity. Most web browsers perform server authentication automatically; the user is notified only if the authentication fails. The authentication process between the server and the client is performed

using the SSL/TLS protocol. Digital certificates are authenticated, issued, and managed by a trusted Certification Authority (CA).

- *(WG350: CAT II) The SA or Web Manager will ensure a DoD PKI certificate is installed and configured for each private web site.*

- *(WG355: CAT II) The SA or Web Manager will ensure a private web server's list of CAs considered trusted is limited to those with a trust hierarchy that leads to the DoD PKI Root CA or to an approved External Certificate Authority (ECA) or are required for the server to function.*

NOTE: There are non DoD roots that must be on the server in order for it to function. Some applications, such as anti-virus programs, require root CAs to function.

Refer to *Appendix B, Server Certificates*, for information on how to obtain personal certificates and server certificates.

3.13 SSL/TLS

SSL/TSL v3.0 and its successor SSL/TLS v3.1 are protocols that provide data security between application protocols such as HTTP (the protocol used by the Web) and the networking protocol TCP/IP. TLS establishes a secure, encrypted connection between the server and a TLS-capable browser, and then encrypts and decrypts information as it is sent and received. SSL v3.0 and earlier versions are not NIST FIPS 140-2 validated for FIPS mode use. TLS or SSL v3.1 is NIST validated for FIPS Mode use; therefore, TLS or SSL v3.1 is the required protocol for encrypting HTTP sessions. The TLS protocol does provide a mechanism that allows for backward compatibility.

By encrypting data, TLS provides confidentiality and assurance that transactions are private and that information has not been altered during transmission. TLS can also authenticate the server to the browser by providing the server's certificate to the browser. The browser must be capable of using the TLS protocol, including verifying certificates and encrypting and decrypting messages. Several browsers (such as Internet Explorer, Netscape Navigator, and FireFox) support TLS. TLS is an open, non-proprietary protocol providing the following services:

- Mutual Authentication	Identities of both the server and clients are authenticated through exchange and verification of their certificates.
- Privacy	All traffic between the server and the client is encrypted using a unique session key.
- Integrity	TLS protects the contents of messages exchanged between server and clients from being altered while in transit.

All sensitive WWW applications will use at a minimum 128-bit SSL v3.1/TLS encryption and will migrate to PKI. In accordance with the *DoD 8520.2 Instruction*, all private web servers will have Class 3 PKI server certificates.

- *(WG340: CAT II) The SA or Web Manager will ensure private web servers use SSL v3.1/TLS to provide encrypted sessions.*

- *(WG342: CAT II) The SA or Web Manager will ensure public web servers that use SSL must use SSL v3.1/TLS to provide encrypted sessions.*

3.14 Symbolic Links

As a rule, symbolic links confuse the system administration task and thus constitute poor practice. Also, there are numerous vulnerabilities related to applications which misuse links to temporary files as part of their installation or during the use of the application itself. Symbolic links allow a user who has accessed the system document tree, to access or create additional documents elsewhere in the system's file structure that are available for web access.

- *(WG360: CAT III) The SA will ensure symbolic links are not used in the web document (content) directory tree.*

NOTE: The .nsconfig file in some versions of Netscape web server software, if used, is exempt from this restriction.

4. WEB SCRIPTS AND PROGRAM SECURITY

4.1 General

There are two types of web pages, static and dynamic. Static pages contain content that is displayed to the web user; no interaction with the web page is involved after it is displayed. Dynamic web pages accept and retrieve information from the web user, produce specialized or customized content, query databases, and generate web pages. This is accomplished via scripting embedded in a web page. Dynamic web pages/web applications must comply with the Application Security Checklist.

Scripts are programs often written in a contemporary computer language. In the context of web technologies, scripting is recognized as an effective and efficient means for implementing both client and server side actions via the web server. Because of the nature of scripting languages, scripts can be very powerful and their use must be monitored with the same diligence as a program. The term "program(s)" in this document applies to both scripts and programs.

In the case of scripts and programs developed by web authors and developers, certification by the local configuration control board (CCB) or technical group is required. The local CCB or technical group will follow the security review guidance provided in the *Application Security and Development STIG and checklist,* before certifying a program for use on a web server.

Web developers and authors will not be allowed to install their own programs, regardless of the programming or scripting language used. (Refer to *Section 2.1, Web Server Security Administration*.)

Interactive programs (e.g., CGI, JavaScript, JScript, PERL, VBScript, asp, aspx) will not be installed on a web server without the knowledge and consent of the Web Manager. (Refer to *Section 2.1, Web Server Security Administration.)*

- *(WA130: CAT II) The IAO will ensure a local CCB, PM, or technical group reviews all programs and scripts before implementing them on the production web server.*

- *(WG370: CAT II) The IAO will ensure the Web Manager does not configure /bin/csh as a viewer for documents of type application/x-csh, application/x-sh, application/csh, or application/sh on the UNIX server.*

- *(WG380: CAT II) Web Managers or SAs will ensure vulnerable programs, such as those detected by security scanning systems, are removed from the server.*

NOTE: Examples of vulnerable scripts and programs include the following:

- *TextCounter Versions 1.0 - 1.2 (PERL) and 1.0 - 1.3 (C++)*
- *guestbook.cgi*
- *bndform.cgi*
- *Cachmgr.cgi*
- *Classified.cgi*

- *Count.cgi*
- *dumpenv.pl*
- *Excite Web Search Engine*
- *mail-lib.pl*
- *Glimpse (PERL scripts) Web Search Engine*
- *info2www, Versions 1.0-1.1*
- *Webdist.cgi*
- *php.cgi*
- *files.pl*
- *nph-test-cgi*
- *nph-publish*
- *FormMail (PERL scripts)*
- *"phf" phone book script*

Executables specific to Windows platform :

- *ntalert.exe*
- *sysloged.exe*
- *tapi.exe*
- *20.exe*
- *21.exe*
- *25.exe*
- *ecware.exe*
- *nc.exe*
- *80.exe*
- *139.exe*
- *1433.exe*
- *1520.exe*
- *26405.exe*
- *i.exe*
- *newdsn.exe*
- *notworm*
- *readme.exe*
- *Wink<random characters>.exe*

4.2 CGI Programs

CGI is a standard for interfacing external applications with information servers, such as HTTP or web servers. The definition of CGI as web-based applications is not to be confused with the more specific .cgi file extension. CGI applications can be written in most programming language. Common applications involve acquiring data via a web page and the browser, executing the CGI application, and returning customized web content. There is a possibility of compromising security when using CGI. Compromise can occur when invalid input is used to build file names, cause a buffer-overflow, or to invoke system commands. Malicious users can provide input data (via a browser) to cause the CGI program to execute an arbitrary system command with the intent of crashing the server or producing erroneous web pages. The intent is to use this feature in a manner unintended or unanticipated by the developer or author of the

program. CGI programs that are carelessly written can grant the malicious user as much access to the server as a privileged account. CGI programs can be written in such languages as PERL, C, C++, shell (sh, ksh, bash, bat), JavaScript, JScript, PHP (PHP: Hypertext Preprocessor), and Windows Script(ing) Host, VBScript, C#, or Java. Each CGI program, that writes files to the server, will use a common directory for temporary files and once that task is completed, the temporary file will be deleted.

- *(WG400: CAT II) The SA or Web Manager will ensure all CGI programs are placed in a designated (e.g., cgi-bin or equivalent) directory. This directory is owned by a non-privileged user account with permissions of owner: read/execute, group: execute, other: none (510), or more restrictive.*

- *(WG410: CAT II) The SA or Web Manager will ensure all CGI programs are owned by the non-privileged user running the web server and have proper access controls.*

- *(WG420: CAT II) The SA or Web Manager will ensure all CGI programs that are backups or otherwise non-operational do not exist in CGI designated directories.*

- *(WG430: CAT II) The SA or Web Manager will ensure CGI directory contents and programs are not available to external FTP clients.*

- *(WG440: CAT II) The SA or Web Manager will ensure all CGI programs are included in the set of files that are checked by a security monitoring software for modification.*

- *(WA032: CAT III) The Web Manager will ensure all CGI programs used on the web server are documented, to include the language used and aim of the program, and that documentation is provided to the IAO.*

4.3 Unvalidated Input

Hyper Text Markup Language (HTML) includes the ability to display selection lists, limit the length of fields to a specific number of characters, embed hidden data within forms, and specify variables provided to CGI programs. This is a great help in reducing how much error checking must be included in programs. Checks for errors from input, whether intentional or accidental, are essential because the anonymous web user can run a CGI program by simply accessing a URL. The IAO will verify that error checking is performed on all input data.

In general, a CGI script will never accept input if any of the following exists:

- Any cookie or special tag not created by the server
- Input that exceeds the maximum length of the defined variable
- A non-alpha and non-numeric character where such characters will be used in the formation of system commands or file names, without specifically checking for and allowing such characters (e.g., quotes, tick marks, slashes, and asterisks).
- Values that are outside the defined scope of the expected value
- Microsoft Office Attachments

- Characters in dynamic elements (i.e., < > % # " ' ( ))
- HTML input

- *(APP1020: CAT II) The IAO will ensure the application adequately validates user inputs before processing them.*

4.4 Mobile Code

Mobile Code is the term given to software modules obtained from remote systems outside the enclave boundary and then downloaded and executed on a local system without explicit installation or execution by the recipient.

For additional policy guidance and usage restrictions see *Assistant Secretary of Defense (C3I) Memorandum, Subject: "Policy Guidance for use of Mobile Code Technologies in Department of Defense (DoD) Information Systems," 7 November 2000* and DoD Instruction 8500.2, February 6, 2003.

4.5 PERL Scripts

Practical Extraction and Report Language (PERL) is an interpreted language optimized for scanning arbitrary text files, extracting information from those text files, and printing reports based on that information. The language is often used in shell scripting and is intended to be practical, easy to use, efficient, and complete. Unfortunately many widely available freeware PERL programs (scripts) are extremely insecure. This is often the result of not checking user input to a form. The safeguards noted in *Section 4.3, Improper Input*, also apply to PERL.

PERL has a mechanism (taint) that protects the system from a variable that has been set from outside the program. When the data is *tainted*, it cannot be used in UNIX and C programs such as eval(), system(), exec(), pipes, or popen(). The script will exit with a warning message.

- *(APP1020: CAT II) The IAO will ensure the application adequately validates user inputs before processing them.*

- *(WG460: CAT II) The SA or Web Manager will ensure if PERL is being used in a Web context the taint (-t) input validation-checking mechanism is used.*

For PERL Version 5, taint checking is built in and is enabled by passing the –T switch to the PERL interpreter (e.g., #!/usr/local/bin/perl -T).

For Apache 1.2 and later, provided mod_perl is installed, the directive PerlTaintCheck on can be used to enable the Perl taint option for all Perl scripts.

For Apache 2.x users, provided mod_perl is installed, enable Perl taint mode checking using the following option: PerlSwitches –T.

4.6 JavaScript

JavaScript is a scripting extension of HTML. JScript is the Microsoft equivalent of JavaScript. It extends the ability of the server to respond to client events without the need for client/server communications. JavaScripts cannot exist outside of HTML code. To function, JavaScripts must be embedded in a Web page. However, server-side statements that connect to databases or access the file system on the server can exist. JavaScripts is an interpreted language designed for controlling the browser. It has the ability to open and close windows, manipulate form elements, adjust browser settings, and download and execute Java applets. (Applets are mini application modules embedded in web pages [e.g., for animating a picture].) JavaScript is an object-oriented programming language used to create stand-alone applications and applets. JavaScripts that are improperly written can make the server vulnerable to outside attack by allowing unauthorized access to sensitive server system or data files. JavaScript code can be easily manipulated and Java applets can be readily de-compiled.

4.7 Java Applications

Despite the similarity of name, Java and JavaScript are two separate entities. Java is a language designed by Sun Microsystems expressly for use in the distributed environment of the Internet. Java contains a series of interlocking defenses that are in four layers:

- The language is designed to be safe, and the Java compiler ensures that the source code does not violate default security rules.
- All bytecode executed by the runtime modules is screened to ensure they obey the rules.
- The class loader ensures that classes do not violate name space or access restrictions.
- Application Program Interface (API) specific security prevents applets from performing destructive activity.

Java code may be used on DoD information systems if it is obtained from a trusted source. The resultant Java code may be in the form of a Java applet or Java application. By default, Java applets are restricted to functioning in a “sandbox” as implemented by the web browser. Java applications on the other hand may be designed to exploit any resource on a computer system.

- *(WG490: CAT III) The SA or Web Manager will ensure only Java programs such as bytecode, class files, and virtual machine types reside on the server.*

NOTE: In the case of mainframe systems, the IBM Resource Access Control Facility (RACF) provides another layer of protection against malicious use of the JDK.

4.8 Java Servlet Engines and Java Server Pages

This combination of methods and technologies, Java Servlet Engines and Java Server Pages, builds on the CGI standard and makes that standard easier to use. The servlet engine loads Java classes to create a servlet instance when the request arrives from a Java Server Page.
Java Servlet technology provides Web developers with a mechanism for extending the functionality of a web server and for accessing business systems. A servlet can be thought of as

an applet that runs on the server side. Over 25 servlet engines are available to extend the functionality of web servers.

Servlets provide a component-based, platform-independent method for building web-based applications, thus they will be found in all operating system environments. Unlike proprietary server extension mechanisms (such as the Netscape Server API or Apache modules), servlets are server- and platform-independent.

JavaServer Pages (JSP) technology enables rapid development of web-based applications that are platform independent. JSP technology separates the user interface from content generation enabling designers to change the overall page layout without altering the underlying dynamic content.

When using Java Servlets Engines or Java Server Pages, any sample files that accompany the product's installation will be removed.

4.9 JAVA 2 Enterprise Edition (J2EE)

J2EE is a specification for developing enterprise and distributed applications from JavaSoft (Sun Microsystems). J2EE encompasses a large set of technologies: JavaServer Pages (JSP), Servlets, Enterprise JavaBeans (EJB), JDBC Java Naming and Directory Interface (JNDI), Java Messaging, Java Transaction Support, JavaMail and Java support for CORBA and support for extensible markup language (XML).

J2EE is a specification, not a product. Multiple vendors have created platforms to develop and deploy J2EE environments including IBM's WebSphere, BEA's WebLogic, and others.

J2EE applications are made up of components that can be deployed into different containers. These components are used to build a multi-tier enterprise application. For example, you may have a Web-tier, EJB-tier or Application-tier. A container provides security in two forms: Declarative and Programmatic. The goal of the J2EE security architecture is to achieve end-to-end security by securing each tier. The J2EE specification assumes that a J2EE application will be integrated into an existing security architecture that implements authorization, encryption, and security for the overall platform.

4.9.1 Declarative Security

Declarative contracts are contracts between those who develop and assemble application components and those who configure applications in operational environments. In the context of application security, application providers/programmers are required to declare the security requirements of their applications in a document called a "deployment descriptor". This deployment descriptor is used to derive a security policy for use by a component's container. An application deployer then uses container-specific tools to map the application requirements that are in a deployment descriptor to security mechanisms that are implemented by J2EE containers.

Declarative security refers to an applications security structure including security roles, access control, and authentication requirements. These requirements are external to the application

meaning the container provides the security not the application itself. Changes to the security policy can be made here without changes to the underlying JSP or JAVA code.

The J2EE specification focuses primarily on authorization within J2EE components.

4.9.2 Programmatic Security

Programmatic security refers to security decisions that are made by security-aware applications. In this case, the application not the container provides security. Programmatic security tends to be less portable in that if a security policy changes every component must be checked or changed depending on the security requirements in the current security policy.

4.9.3 Realms, Principals, Roles, and Role References

The J2EE specification focuses on authorization within the J2EE components for its primary security. The J2EE specification defines security terms that can be used to integrate security mechanisms with host systems that have diverse authentication mechanisms. These terms are Realms, Principals, Roles, and Role References.

4.9.3.1 Security Realms

A security realm is a J2EE security policy domain. This defines the way in which a user is authenticated to a component. J2EE supports Basic HTTP (the HTTP realm), HTTP Digest Authentication, Form-based authentication, and Client-certificate authentication.

- *(WG345: CAT II) The IAO will ensure if Basic HTTP or Form-based authentication is used, TLS is used to encrypt the authentication traffic.*

4.9.3.2 Principals

A principal can be any entity that can be authenticated by an authentication protocol to the security service. A principal can be a user although the J2EE does not require the principal name to be the same as the user's login name.

4.9.3.3 Roles

A role is a definition of the way a user will use the system, however, a role covers only a specific application or component in a J2EE server. Typical roles will be user, administrator, manager, developer, researcher, and so on. Each of these user categories is called a security role, an abstract logical grouping of users that is defined by the person who assembles the application. Assigning users to one or more authentication groups or granting privileges to users accounts usually implement a role. When an application is deployed, the deployer will map the roles to security identities in the operational environment.

4.9.3.4 Role References

A role reference is the name of a role used within the code of a J2EE application. As part of the J2EE application environment definition, the deployment descriptor, every role reference must

be mapped onto a real role. The abstracting of the coded role reference from the actual role helps improve portability of a J2EE component.

4.10 Server Side Includes (SSIs)

SSIs are a specialized form of HTML comment that allows the web server to provide web pages updated with current content. This is done by examining files with an extension of shtml (or any other extension requested), and replacing SSI commands with the results of the evaluation of those SSI commands that reveal details about the server configuration and provide the results serving the page to the web user or requester. The capability for SSIs to execute shell commands and programs will be disabled in the web server software.

- *(WG200: CAT I) The SA or Web Manager will ensure access to the directory tree browser, the shell, or other operating system functions and utilities is restricted to administrators.*

In IIS, this setting is controlled by a radio button in the Application Settings section of the Properties/Home Directory dialog box of the web site or simply by removing the mapping to the file type shtm or shtml. In Apache web servers, the use of <exec cgi> is not permitted as this allows the execution of a file anywhere in the file system.

4.11 Security Settings for Windows Script Host (WSH)

Originally, WSH, sometimes referred to as Windows Scripting Host did not include any mechanism for preventing the execution of WSH scripts from untrusted sources. This led many users to mistakenly assume that nothing could be done to protect a system against infection from WSH script viruses. All 32-bit Microsoft Windows operating systems contain mechanisms to protect a system against accidental infection from email attachments or malicious HTML pages containing viruses.

An SA can prevent scripts from being executed without removing WSH functionality from the system. An SA can also specify that this behavior be valid only for certain users or for the whole system. This option is available in all 32-bit versions of Windows, but it must be activated. The way to block WSH scripts from executing differs between operating systems (i.e., between Windows 2000/2003 and Windows NT 4).

In Windows 2000/2003 and Windows NT 4, the right to execute a file can be limited to specific user groups; so ordinary users can be blocked from executing WSH EXE files by following these steps:

1. Log on as an Administrator, and search for the files CScript.exe and WScript.exe (in the \System32 folder).
2. Right-click on each file, and choose Properties from the Context menu.
3. Click on the Security property page, click Everyone or IUSR_machinename, and uncheck Read & Execute in the Allow column.

Repeat these steps for all other user groups for which WSH is to be disabled. (Only the System and Administrator accounts have the right to execute a script. This implies the installation of Windows on an NTFS volume.)

After closing the Security property page, execution of WSH scripts is blocked for the specified users or user groups. To execute a script, log on as Administrator and execute the file.

In Windows 2000/2003, a System Administrator can use the MMC to specify applications that a user is not allowed to execute. If WScript.exe and CScript.exe have been specified, the user cannot execute scripts after the next logon.

Per *Section 4.4, Mobile Code*, Windows Script Host is a Category 1 mobile code technology. As such, its use is limited to local programs and command scripts for use by the SA or Web Manager. The SA will assure that only privileged users (e.g., SA or Web Manager) have full control permissions to WScript.exe and CScript.exe.

- *(WG470: CAT II) The SA will ensure Wscript.exe and Cscript.exe access is restricted to Administrative accounts.*

4.12 ASP.NET and Open Network Environment (ONE) Web Services

The Internet is evolving from web sites that just deliver user interface pages to browsers to a generation of programmable web sites that directly link organizations, applications, services, and devices with one another. This linkage is intended to be system architecture independent. These resulting "programmable web sites" are intended to become more than passively accessed sites; they become user controlled web services. In this context, ASP.NET is a programming framework (formerly known as Active Server Pages) that can enable this new vision for web services. The SUN counterpart to ASP.NET is ONE, a predominantly Java environment.

The common language runtime provides built-in support for creating web services, using a programming abstraction that is consistent and familiar to both ASP.NET Web Forms developers and existing Visual Basic users. The resulting model is both scalable and extensible, and embraces open Internet standards (HTTP, XML, Simple Object Access Protocol (SOAP)), Web Service Description Language (WSDL) (see *Section 5, Security of Other Web Related Services*, in this STIG) so that it can be accessed and consumed from any client or Internet-enabled device.

ASP.NET Web Forms pages are text files with an .aspx file name extension. They can be deployed throughout an IIS virtual root directory tree. When a browser client requests .aspx resources, the ASP.NET runtime parses and compiles the target file into a .NET Framework class. This class can then be used to dynamically process incoming requests.

NOTE: The .aspx file is compiled only the first time it is accessed; the compiled type instance is then reused across multiple requests.

By taking an existing HTML file and changing its file name extension to .aspx (no modification of code is required) an ASP.NET page is created. ASP.NET also provides support for web services with the .asmx file. An .asmx file is a text file that is similar to an .aspx file. These files can be part of an ASP.NET application that includes .aspx files.

5. SECURITY OF OTHER WEB RELATED SERVICES

5.1 FTP

FTP is a commonly exploited service that should not be installed on a server that also provides web publishing services, email, or database services. In some cases, FTP servers invoke parameters for other system utilities, such as tar in UNIX, without checking the validity of the parameters input by a user. This compounds the vulnerability.

FTP is primarily a tool for transferring large files or simply to provide a repository of files for users to view and download. However, there are serious security problems associated with FTP. First, FTP can allow anonymous login and/or logons using local or domain user accounts, a major back door into systems if it is enabled. Second, FTP is a non-encrypted protocol that transmits logon user IDs and password in clear text. Third, under Windows 2000 and 2003, FTP logons are not subject to account-lockout restrictions.

FTP is designed to do the following:

- Promote the sharing of files (computer programs and/or data)
- Encourage indirect or implicit (via programs) use of remote computers
- Shield a user from variations in file storage systems among hosts
- Transfer data reliably and efficiently

Because FTP is a non-encrypted protocol that transmits user IDs and passwords in clear text, it would be easy for a malicious user to sniff packets off your Internet link looking for user accounts and passwords, or to initiate a brute-force attack against a known user account without fear of that account being locked out. If permissions on the FTP content directory are not correctly set, the malicious user could transfer files and utilities of his choosing for execution on the targeted server.

Solutions to the problems outlined above include the following:

- Avoid using FTP if possible
- If file transfer is necessary, configure an FTP server on a standalone system with no valuable data stored on it
- Look for a secure file transfer solution, such as using HTTP 1.1 and SSL, for file transfer via Web sites
- Audit access to your FTP root and server in general

- (*WFTP020: CAT III) The IAO will ensure FTP write access is restricted to administrators and authorized authors.*

- *(WFTP040: CAT II) The IAO will ensure anonymous FTP is not permitted on a "private" web server.*

- *(WFTP060: CAT II) The IAO will ensure FTP use of a secure file transfer solution (e.g., SSH) is restricted.*

5.2 SMTP

SMTP is the cornerstone of messaging interoperability across the Internet. The original protocol was simple and concentrated on the task of sending 7-bit plain text messages across an IP link between a client and a server. Port 25 is the default port for all SMTP operations.

SMTP has evolved to incorporate the changes that today's messaging environment requires. Extended SMTP (ESMTP) and Multimedia Internet Mail Extension (MIME) are the two major advances that have enabled SMTP to deliver highly functional messaging systems.

A proven mail program that does not use shell escapes may be used on a web server. In the UNIX environment, if sendmail is used by a CGI program, the program /usr/lib/sendmail will be used. The programs /usr/bin/mailx or /usr/bin/mail will never be used to send mail because these mail programs allow shell escapes.

In the Microsoft product arena, a web-based email solution can be accomplished via Outlook Web Access (OWA) in Exchange 2000 and Exchange 2003. IIS must be installed for OWA to function. It handles the incoming HTTP requests from web browsers and sends HTTP responses to an Exchange Server or OWA server.

- *(WG330: CAT II) The SA will ensure a public web server is only capable of processing outbound e-mail.*

NOTE: A public web server will not process inbound e-mail.

- *(WG347: CAT II) The SA or Web Manager will ensure an email service accessible via a web browser utilizes HTTPS (TLS) security to encrypt sessions.*

5.3 Web Services

Web Services is the term used to convey the notion of *conversations* or *transactions* that can take place over the Internet between applications. From an enterprise viewpoint, this is a powerful concept. Implicit in this paradigm is the notion that applications for invoicing a bill of materials will interact directly with partner systems and produce orders and shipping manifests without the need for human involvement. In this context, a web service is any service that satisfies these three conditions:

- Available over the Internet
- Uses a standard messaging system
- Not tied to any one OS or programming language

Web Services incorporate several technologies and protocols to achieve these transactions. The XML is the data format/language by which these different applications record data. SOAP is the method by which the XML file is transported over HTTP, HTTPS, or SMTP. WSDL is the means to describe a web service beyond the XML schema. Universal Data Description Language is a means of advertising the web service. WS-Security describes several security

methods by which the SOAP message can be secured. The Web Services Interoperability Group has developed WS-Security.

The technologies and languages standards discussed in this section have been adopted or are in the process of adoption by the Organization for the Advancement of Structured Information Standards (OASIS) and the WWW Consortium (W3C). Both organizations serve as the standard for Web Services technologies. These technologies are defined or can be defined in schema format and each has a representative name space which defines its format standard.

The term, *web portal*, is also used in this context to describe a sophisticated dissemination of document, search, and other interface features available to users in a distributed manner over the Internet. Typically, the application components will be distributed across the Internet and not reside on a single server or even a single network. The data exchanges in this environment are designed to be automatic and more efficient than the traditional model of the human (manual) involvement process of Web browser requests to a web server.

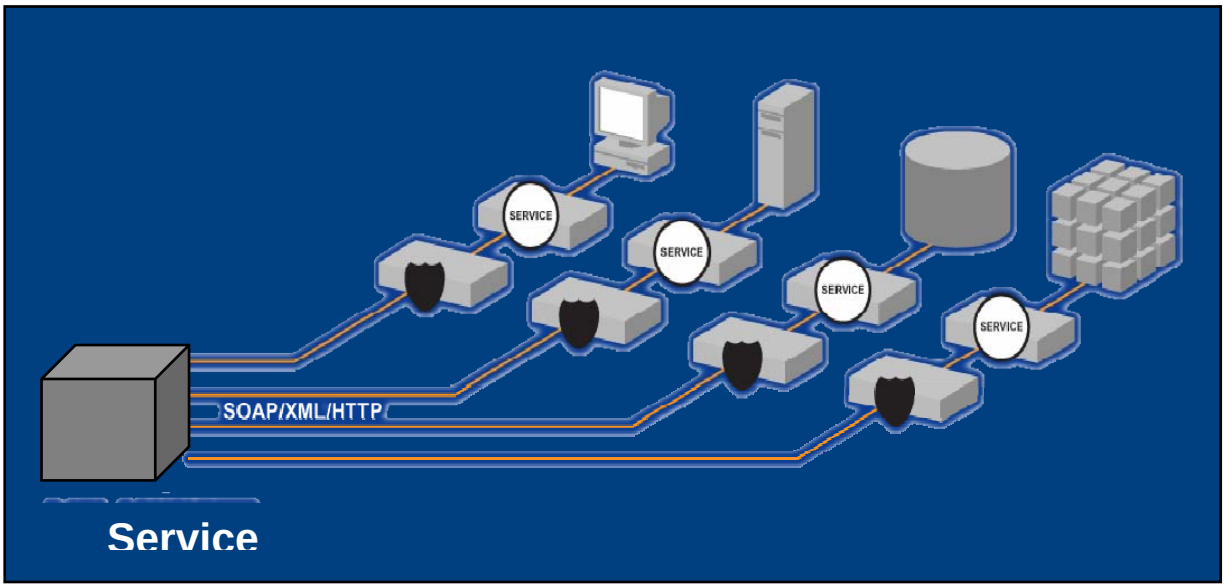

Figure 5-1. Basic Web Services Architecture

In this scenario a request is made via a web services portal (the SERVICE). The portal, in turn, sends the request to the appropriate services using SOAP to transport the XML over HTTP. Not shown is the opportunity for each independent service to interact with the others. This allows for platform independence and data transfer without user intervention.

5.3.1 XML

HTML is about displaying information; XML is about describing information or creating metadata, that is data about data. XML is a standard language used to structure and describe data that can be understood by different applications. XML enables diverse computer systems to share data, regardless of operating system and programming language. The data of an XML file is described in an XML Schema. This schema defines the data structure and format of the XML

file. XML, while designed to provide interoperability among application components on the Web, is intended to work in many environments outside the Web, including publishing, data interchange, and commercial e-commerce applications. Finally, XML utilizes HTTP/HTTPS as a transport, allowing remote method requests and data to pass through enterprise firewalls via standard ports, such as 80/443.

Existing secure web standards, such as HTTPS and SSL/TLS, are not able to address XML specific issues such as partial document signing and the fact that XML documents are often processed in stages along loosely coupled network paths. To solve these problems, developers will use XML Encryption to encode individual parts of the XML document; XML Signature to manage the integrity of XML as it moves through the web, again along loosely coupled network paths, and XML Key Management Specification to deal with PKI verification and validation.

5.3.1.1 XML Digital Signature (DSIG)

XML DSIG is a way of ensuring integrity of a document. SOAP messages, wholly or in part, are first digested. The digest is a hash value equivalent to a human fingerprint. The digest, along with other sensitive data, is then digitally signed using the sender's private key and then encrypted using the receiver's public key. Because the signature is encrypted using the receiver's public key, only the receiver can decrypt it and verify the signature and message digest. Any tampering during the transmission will lead to a signature/hash verification failure.

5.3.1.2 XML Data Encryption

Sensitive data can also be encrypted using either session keys or a public/private key. Even with the message sent in the clear, the part that is encrypted will be opaque and difficult to crack. The W3C draft, XML Encryption, defines the process and format of the encrypted XML data. Both the request and response of a SOAP method are signed and verified by the SOAP client and server. In addition, any parameter values are encrypted before sending to server; and the returned values from the server are also encrypted.

5.3.2 SOAP

SOAP is used to send XML-based unencrypted or encrypted commands and XML messages. SOAP has been described as an envelope for XML. SOAP runs on top of HTTP and thus inherits the security holes common to HTTP implementations. SOAP conveys XML messages and is designed to pass through firewalls as HTTP, HTTPS, and SMTP. In doing so, SOAP uses standard HTTP methods such as POST. Developers will define in the application permissions and rights that specify who and what has access to data, executable components, and system resources. SOAP transactions/messages can be strongly protected through digital signature and encryption.

Users of SOAP services can be authenticated in many different ways including token-based authentication and digest authentication. Token-based authentication requires users to supply credentials through a secure channel. SOAP servers respond with a token that can be used for all subsequent requests.

An example of using SOAP to send basic credentials to be used in identification and authentication is:

```
<S:Envelope>
xmlns:S=http://www.w3.org/2001/12/soap-envelope
xmlns:ws=http://schema.xmlsoap.org/ws/2002/04/secext>
        <S:Header>
        <ws:Security>
        <ws:UsernameToken>
                <ws:Username>Name</ws:Username>
                <ws:Password>password</ws:Password>
        </ws:UserToken>
        </ws:Security>
        </S:Header>
</S:Envelope>
```

5.3.3 WSDL

Where the XML Schema leaves off the WSDL file picks up. WSDL is a specification defining how to describe web services in a common XML grammar. WSDL describes four critical pieces of data:

- Interface information describing all publicly available functions
- Data type information for all message requests and message responses
- Binding information about the transport protocol to be used including ports
- Address information for locating the specified service

WSDL represents a contract between the service requestor and the service provider, in much the same way that a Java interface represents a contract between client code and the actual Java object. The crucial difference is that WSDL is platform and language independent and is used primarily (although not exclusively) to describe XML based Web Services.

5.3.4 Universal Discovery Description Integration (UDDI)

UDDI is the discovery layer within the web services protocol stack. UDDI is a technical specification for publishing and locating businesses and web services. Step one of UDDI is the building of a distributed directory or a registry of businesses and web services.

UDDI has been described as the Yellow Pages of web services or a directory of web services and their descriptions. A UDDI entry is an XML file that describes a business and the services it offers. A UDDI entry may contain three parts: The White Pages, The Yellow Pages and The Green Pages. The White Pages describes the business, name, address, and contacts. The Yellow Pages describes the type of business or industry. The Green Pages describe the web service interface. This includes a document called the Type Model or tModel. The tModel usually includes a WSDL file.

NOTE: It should be noted that there is a potential downside to organizations publishing directory information to the UDDI. Organizations need to ensure that sensitive information about their organization is not published to the UDDI as this may lead to sensitive information about their organizations web services descriptions and network addresses being made public.

5.3.5 WS-Security

WS-Security is the foundation for all other web services security specifications. It is the fundamental way to add security to SOAP messages. WS-Security defines extensions to SOAP that provide for token passing and provides for end-to-end message level security. WS-Security describes enhancements to SOAP messaging to provide quality of protection through message integrity, message confidentiality, and single message authentication. WS-Security also provides a general-purpose mechanism for associating security tokens with messages. No specific type of security token is required by WS-Security. It is designed to be extensible (e.g., support multiple security token formats).

Additionally, WS-Security describes how to encode binary security tokens. Specifically, the specification describes how to encode X.509 certificates and Kerberos tickets as well as how to include opaque encrypted keys. It also includes extensibility mechanisms that can be used to further describe the characteristics of the credentials that are included with a message.

SOAP Example Using x509 Certificate:

```
<WSSE:Security
xmlns:wsse=http://schemas.xmlsoap.org/wd/2002/12/secext>
<wsse:UserNameToken>
        <wsse:Username>”Name”</wsse:Username>
        </wsse:UsernameToken>
</wsse:Security>
```

5.3.6 Security Assertions Markup Language (SAML)

SAML is designed to facilitate the secure exchange of authentication and authorization information between partners regardless of their security systems or e-commerce platforms. It establishes assertion and protocol schemas for the structure of the documents that transport security. It provides a standard way to define user authentication, authorization and attribute information in XML documents.

The main components of SAML include the following:

Assertions: SAML defines three kinds of assertions, which are declarations of one or more facts about a user (human or computer). Authentication assertions require that the user prove his identity. Attribute assertions contain specific details about the user, such as his credit line or citizenship. The authorization decision assertion identifies what the user can do (for example, whether he is authorized to buy a certain item). Request/response protocol: This defines the way that SAML requests and receives assertions. For example, SAML currently supports SOAP over

HTTP. In the future, the SAML request and response format will bind to other communications and transport protocols.

Bindings: These detail exactly how SAML requests should map into transport protocols such as SOAP message exchanges over HTTP.

Profiles: These dictate how SAML assertions can be embedded or transported between communicating systems.

- *(WG344: CAT II) The IAO will ensure SAML assertions are encrypted using SSL v3.1 / TLS security.*

5.4 Collaboration (Message Board) Servers

Web message board and collaboration servers are powerful and easy to use tools accessible via a web browser. Web message board servers foster communication in corporate intranets, extranets, educational institutions, and departmental workgroups.

The Standard Version of Web Message Board Servers holds up to 100 boards and also includes chat features. Advanced versions of these servers are tailored for large communities and contain unlimited boards, enhanced management tools, and enterprise level database support.

Principal uses for web message board servers are as follows:

- Mailing list
- Customer service/technical support
- Online education
- Project collaboration
- Virtual meetings
- Foreign-language conferences

Such servers must be approved for use by the DAA. If so approved, the following security measures will be followed.

- *(WG070: CAT III) The IAO will ensure all web message board and collaboration servers are implemented behind a firewall.*

- *(WG346: CAT II) The SA or Web Manager will ensure web message board and collaboration servers employ SSL/TLS to encrypt traffic.*

5.5 LDAP Server Security

LDAP is an open network protocol standard designed to provide access to distributed directories. LDAP provides a mechanism to query or modify information that exists in a directory information tree (DIT). A DIT may contain a broad range of information about different types of objects that might include users, printers, applications, and other network resources.

By default, the LDAP Directory server will permit anonymous access (i.e., read, search, compare only) to all data in the directory. The Access Control Instruction (ACI) that controls access to data in the directory server cannot be edited or removed permanently. Fortunately, the Deny permission overrides the Allow permission, thus creating an ACI that denies access to data in the Directory server.

- *(WL195: CAT I) The SA or Web Manager will ensure the anonymous user does not have access to the LDAP Schema.*

- *(WL200: CAT I) The SA or Web Manager will ensure the anonymous user does not have access to directory content beyond that needed to authenticate.*

- *(WL205: CAT II) The SA or Web Manager will ensure all administrative connections to the LDAP server are encrypted.*

- *(WL210: CAT II) The SA or Web Manager will ensure all connections between the web server and LDAP server are encrypted.*

5.6 Web Proxy Servers

A Web proxy server has two network adapters, one cabled to the NIPRNet and one cabled to the internal network DMZ. The proxy server software intercepts each inbound or outbound NIPRNet message and subjects it to scrutiny before handing the message to the other network adapter. The proxy server can distinguish between legitimate incoming messages which are responses to browsing the web site and illegitimate incoming messages that were not requested by the web server (i.e., hacking attempts). The software can also use Network Address Translation (NAT) to substitute a hidden, internal IP address for the web server's publicly known Internet IP address.

A Web proxy server offers different levels of security, including packet level, circuit level, and application layer (looking inside content). It supports all significant networking transport protocols and can operate as a dedicated firewall, dedicated cache, or combination firewall/cache. A web proxy server-protected network can contain both Windows and non-Windows web servers.

- *(WG550: CAT II) The IAO will ensure a web proxy server filters Internet requests at the application network layer.*

- *(WG560: CAT II) The IAO will ensure all connections to Enclave level proxy servers are authenticated.*

5.7 Wireless Enabled Web Servers

The Wireless Access Protocol (WAP) is focused on enabling the interconnection of the web server and wireless terminals. All WAP enabled web servers must comply with the DoD Wireless STIG. The goal of WAP is to enable an extremely wide range of wireless terminals, ranging from mass-market mobile telephones and pagers to more powerful devices (i.e., personal

data assistants (PDAs)), to enjoy the benefits of web technology and interconnection. The wireless medium is inherently uncontained, which means that maintaining security can be difficult. When a radio modem transmits information, anyone can potentially intercept that broadcast. Aside from a special order, proprietary solution, WAP phones currently do not support advanced authentication and encryption methods such as SSL or end-to-end Wireless Transport Layer Security (WTLS). There are several vendors that offer WAP-2 compliant gateways (e.g., Neomar, etc.) that provide end-to-end WTLS security so the security protocol translation described below is not necessary). In most cases, these gateways perform the WAP to HTTP translation inside the wireless gateway that is usually located inside a DMZ of the enterprise.

Currently, browser requests sent from a WAP device to WAP enabled web server are sent first as a Wireless Session Protocol (WSP) request to a WAP gateway. Most WAP browsers and gateways support WTLS, which means the data from these devices is sent securely from the device over the air to the WAP gateway. The WAP gateway converts the request to HTTP or HTTPS (the session will be encrypted using SSL) and establishes a session over the Internet.

The same safeguards that now protect the integrity and confidentiality of enterprise data in wired networks also apply to wireless networks. Any wireless solution that promises to extend the reach of enterprise Intranets (LANs) must include technologies that do the following:

- Protect user IDs and passwords from interception by unauthorized users
- Protect corporate data from exposure

Security requirements for WAP enabled web server deployments are as follows:

- *(WA240: CAT III) The IAO/PM will ensure a WAP enabled web server deployment does the following:*

  - *Implements an IPSec policy for secure communications*
  - *Implements HTTPS for secure browsing*
  - *Uses wireless accounts (either auxiliary domain or Access User topologies)*
  - *Isolates the WAP enabled web server in a DMZ*

NOTE: WAP can also refer to the WAP Forum that has introduced a set of protocols optimized for wireless networks that complement existing Internet-standard protocols.

This page is intentionally left blank.

APPENDIX A. RELATED PUBLICATIONS

GOVERNMENT PUBLICATIONS

DoD Directive 8500.1, “Information Assurance,” 24 October 2002.

DoD Instruction 8500.2, “Information Assurance IA Implementation,” 6 February 2003.

DoD Instruction Number 8520.2 issued April 2004 “Public Key Infrastructure (PKI) and Public Key (PK) Enabling.”

DoD Instruction 8551.1, "Ports, Protocols, and Services Management (PPSM)," 13 August 2004.

DISA Memorandum: DISA Web Policy, Enforcement, and Operational Security,
12 March 2003.

DISA World Wide Web Handbook Version 5.0.

DD Web Policy, “Web Site Administration Policies and Procedures,” 25 November 1998 (updated 11 January 2002). (Also see http://www.defenselink.mil/Webmasters, DoD Web Site Administration Policies and Procedures.)

Chairman of the Joint Chiefs of Staff (CJCS) Manual 6510.01, "Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)," 15 March 2002.

Defense Information Systems Agency (DISA) OS/390 Security Technical Implementation Guide, Version 4, Release 1 (2 volumes).

Interim Department of Defense (DoD) Certification and Accreditation (C&A) Process Guidance (DIACAP), 6 July 2006.

Defense Information Systems Agency Instruction (DISAI) 630-230-19, “Security Requirements for Automated Information Systems (AIS),” July 1996.

DISAI 630-255-7, “Internet, Intranet, and World Wide Web,” 6 September 1996.

DISAI 630-230-31, “Enclave Security,” 30 March 2001.

Defense Information Systems Agency (DISA) Naming Convention Standards, February 1996.

DISA Computing Services Security Handbook, Version 3, 1 December 2000.

DISA Application Security Checklist v2 r1.4

DISA Network Infrastructure Security Technical Implementation Guide.

Addendum to the NSA Guide to Securing Microsoft Windows NT Networks and NSA Guides to Securing Windows 2000, Version 43 (to match NSA Guide), Release 1, 26 November 2002.

Defense Information Systems Agency (DISA) UNIX Security Technical Implementation Guide, National Security Agency (NSA), "Information Systems Security Products and Services Catalog" (Current Edition).

National Institute of Standards and Technology (NIST), "Guidelines on Securing Public Web Servers," Special Publication 800-44.

Defense Logistics Agency Regulation (DLAR) 5200.17, "Security Requirements for Automated Information and Telecommunications Systems," 9 October 1991.

AR 25-2, Information Assurance, dated 14 November 2003.

Air Force Systems Security Instruction (AFSSI) 5021, *Time Compliance Network Order (TCNO) Management and Vulnerability and Incident Reporting*, 15 August 1996.

AFSSI 5023, *Viruses and Other Forms of Malicious Logic*, 1 August 1996.

AFSSI 5027, *Network Security Policy*, 27 February 1998.

Secretary of the Navy Instruction (SECNAVINST) 5239.2, "Department of the Navy Automated Information Systems (AIS) Security Program," 15 November 1989.

Navy Staff Office Publication (NAVSO Pub) 5239-15, "Controlled Access Protection Guidebook," August 1992.

Public Law 100-235, 100th Congress, An Act cited as the "Computer Security Act of 1987," 8 January 1988.

Memorandum for Secretaries of Military Departments, et al, "Web Site Administration," 7 December 1998.

Memorandum for Secretaries of Military Departments, et al, "DoD Public Key Infrastructure," 12 August 2000.

Memorandum for Secretaries of Military Departments, et al, "Policy Guidance for the Use of Mobile Code Technologies in DoD Information Systems," 7 November 2000.

OTHER PUBLICATIONS

International Business Machines Corporation

OS/390 HTTP Server Planning, Installing and Using, Version 5.2 (SC31-8903)

OS/390 HTTP Server Planning, Installing and Using, Version 5.3 (SC31-8690)

GENERAL INFORMATION SITES

http://iase.disa.mil	Defense Information Systems Agency Information Assurance
http://www.disa.mil/handbook/toc.html	DISA/NCS World Wide Web Handbook, Version 2
http://www.cert.mil	Department of Defense Computer Emergency Response Team (CERT)
http://www.cert.org	A focal point for the computer security concerns of Internet users
http://csrc.nist.gov/publications	National Institute of Standards and Technology's Computer Security Resource Clearinghouse
http://www.cerias.purdue.edu	Center for Education and Research in Information Assurance and Security (formerly COAST)
http://www.redbooks.ibm.com/	"How to" books, written by very experienced IBM professionals from all over the world
http://www.microsoft.com/technet/security/current.aspx	Microsoft Security Bulletin and Patch Listings
http://www.netscape.com/security/notes/index.html	Netscape Security
http://hoohoo.ncsa.uiuc.edu/cgi/security.html	Writing secure CGI scripts
http://language.perl.com/faq/	PERL FAQ
http://www.ietf.org/rfc.html	RFC Index
http://www.nipc.gov	National Infrastructure Protection Center (an FBI program)
http://www.defenselink.mil/Webmasters	DoD Web Site Administration Policy
http://www.ibm.com/software/Webservers/	IBM HTTP Server documentation
http://java.sun.com/j2ee/tutorial/	Sun JAVA Tutorials and Documentation

http://www.samspublishing.com/	Articles and documents on J2EE Security and other systems
http://www.oasis-open.org	Information Resources on Web Services
http://www.w3.org/	Information and Resources on everything Web
http://www.bea.com	Resource for BEA WebLogic and J2EE framework
https://gesportal.dod.mil/sites/DODPKE	DoD Public Key Enablement Home

APPENDIX B. SERVER CERTIFICATES

B.1 User Certificates

To obtain a user PKI certificate, please contact your local Local Registration Authority (LRA) for specific information. If you are unsure of whom your LRA is, contact your SM or IAM.

B.2 Server Certificates

To obtain a server certificate, connect to the following URL and follow the instructions on the site for requesting a Server PKI Certificate:

http://DODpki.c3pki.chamb.disa.mil

Before requesting a server certificate from the DoD PKI, it is important that the submitted request meets specific guidelines, or it will be rejected. When entering the distinguished name information for your server, adhere to the following guidelines. These are the fields that you need to enter and the values that go with them:

Key Size:	**1024 *only***
Common Name:	The fully qualified hostname of your server (e.g., www.adu.acom.mil)
Organization:	**U.S. Government**
Organizational Unit:	**'C/S/A', ou=PKI, ou=DOD** (where 'Combatant Command / Service / Agency (C/S/A)' is the C/S/A for which the server is used) Bottom of Form 1
Locality:	Leave blank
State:	Leave blank
Country:	**US**

Information and requirements concerning DoD Public Key Enabling (DoD PKE) can be found at http://iase.disa.mil and the GES Portal at https://gesportal.dod.mil/sites/dodpke. Questions concerning specific DoD PKE implementations can be directed to Ask_Rosie@disa.mil.

This page is intentionally left blank.

APPENDIX C. LIST OF ACRONYMS

ACL	Access Control List
ACI	Access Control Instruction
ACP	Access Control Program
AFSSI	Air Force System Security Instruction
AFSSM	Air Force System Security Memorandum
AIS	Automated Information Systems
APAR	Authorized Program Analysis Record
API	Application Program Interface
AR	Army Regulation
C&A	Certification and Accreditation
CA	Certification Authority
CCB	Configuration Control Board
CGI	Common Gateway Interface
CINC	Commander-in-Chief
CIO	Chief Information Officer
CIS	Center for Internet Security
CM	Configuration Management
COAST	Computer Operations, Audit, and Security Technology
COE	Common Operating Environment
COMPUSEC	Computer Security
COOP	Continuity of Operations Plan
COPS	Computer Oracle and Password System
COTS	Commercial Off-The-Shelf
CRL	Certificate Revocation List
DBMS	Database Management System
DCTF	DISA Continuity of Operations and Test Facility
DECC	Defense Enterprise Computing Center (was Defense Megacenter [DMC])
DECC-D	Defense Enterprise Computing Center - Detachment
DES	Digital Encryption Standard
DIACAP	DoD Information Assurance Certification and Accreditation Process
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISAI	Defense Information Systems Agency Instruction
DISN	Defense Information System Network
DIT	Directory Information Tree
DITSCAP	DoD Information Technology Security and Accreditation Process
DLAR	Defense Logistics Agency Regulation
DLL	Dynamic Link Library
DMZ	Demilitarized Zone
DNS	Domain Name Service
DoD	Department of Defense
DoD-CERT	Department of Defense Computer Emergency Response Team (was ASSIST)

DOO	Defense Originating Office
DSIG	Digital Signature
DSS	Digital Signature Standard
DTIC	Defense Technical Information Center
E-mail	Electronic Mail
ESM	Enterprise Security Manager
ECA	External Certificate Authority
FIPS	Federal Information Processing Standards
FRCA	Fast Response Cache Accelerator
FSO	Field Security Operations
FTP	File Transfer Protocol
GID	Group ID
GNOSC	Global Network Operations and Security Center
GWAPI	Go Webserver Application Programming Interface
HFS	Hierarchical File System
HIPAA	Health Insurance Portability and Accountability Act
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transport Protocol
I&A	Identification and Authentication
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
IAW	In Accordance With
IHS	IBM HTTP Server
IIS	Internet Information Server
INFOSEC	Information Security
INFOWAR	Information Warfare
IP	Internet Protocol
IS	Information System
ISP	Internet Service Provider
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ITA	Intruder Alert
JAVA	A programming language
JSP	JavaServer Pages
J2EE	JAVA 2 Enterprise Edition (J2EE)
JNDI	JDBC Java Naming and Directory Interface
JDK	JAVA Development Kit
JRE	JAVA Runtime Environment

LAN	Local Area Network
LCC	Local Control Center
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
MIME	Multi-purpose Internet Mail Extension
MMC	Microsoft Management Console
MOA	Memorandum of Agreement
MTA	Message Transfer Agent
NAVSO	Navy Staff Office Publication
NAT	Network Address Translation
NCSA	National Computer Security Agency
NCSC	National Computer Security Center
NFS	Network File System
NIC	Network Information Center
NIPRNet	Non-classified (but Sensitive) Internet Protocol Routing Network
NIS	Network Information Services
NIST	National Institute of Standards and Technology
NNTP	Network News Transfer Protocol
NOSC	Network Operations and Security Center
NSA	National Security Agency
NSAPI	Netscape Server Application Program Interface
NSO	Network Security Officer
NT	Microsoft Networking Operating System
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
OOB	Out-of-Band
OS	Operating System
OSS	Open Source Software
OWA	Outlook Web Access
PAO	Public Affairs Officer
PC	Personal Computer
PDA	Personal Data Assistant
PERL	Practical Extraction and Report Language
PHP	An HTML preprocessor scripting language
PKE	Public Key Enabling
PKI	Public Key Infrastructure
PM	Program Manager
PPSM	Ports, Protocols, and Services Management
PPS	Ports, Protocols, and Services
POC	Point of Contact
RISSC	Regional Information System Security Cell
RNOSC	Regional Network Operations and Security Center (formerly ROSC)

ROSC	Regional Operations Security Center
SA	System Administrator
SAAR	System Authorization Access Request
SAMI	Sources and Methods Intelligence
SAML	Security Assertions Markup Language
SBU	Sensitive but Unclassified
SDK	Software Development Kit
SECNAVINST	Secretary of the Navy Instruction
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SSL	Secure Sockets Layer
SM	Security Manager
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SOP	Standard Operating Procedure
SRR	Security Readiness Review
SSH	Secure Shell
SSL	Secure Socket Layer
SSO	Systems Support Office
STIG	Security Technical Implementation Guide
TASO	Terminal Area Security Officer
TCB	Trusted Computing Base
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDDI	Universal Description, Discovery and Integration
UID	User ID
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VAAP	Vulnerability Analysis and Assistance Program
VCTS	Vulnerability Compliance Tracking System
VIS	Vendor Integrity Statement
VMS	Vulnerability Management System
VPN	Virtual Private Network
W3C	WWW Consortium
WAP	Wireless Access Protocol
WESTHEM	Western Hemisphere
WSDL	Web Service Description Language
WSP	Wireless Session Protocol
WTLS	Wireless Transport Layer Security
WWW	World Wide Web

XML	eXtensible Markup Language